UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/747,238	12/22/2000	David W. Grawrock	42390P9257	9482

8791 7590 02/28/2005

BLAKELY SOKOLOFF TAYLOR & ZAFMAN
12400 WILSHIRE BOULEVARD
SEVENTH FLOOR
LOS ANGELES, CA 90025-1030

EXAMINER	
DINH, MINH	

ART UNIT	PAPER NUMBER
2132	

DATE MAILED: 02/28/2005

Please find below and/or attached an Office communication concerning this application or proceeding.

Office Action Summary	Application No.	Applicant(s)	
	09/747,238	GRAWROCK, DAVID W.	
	Examiner	Art Unit	
	Minh Dinh	2132	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If the period for reply specified above is less than thirty (30) days, a reply within the statutory minimum of thirty (30) days will be considered timely.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☐ Responsive to communication(s) filed on 27 October 2004.

2a)☐ This action is **FINAL**. 2b)☒ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) 1-28 is/are pending in the application.

4a) Of the above claim(s) 1 is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) 2-28 is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☒ The drawing(s) filed on 22 December 2000 is/are: a)☒ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☐ Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08) Paper No(s)/Mail Date _____.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____.
5) ☐ Notice of Informal Patent Application (PTO-152)
6) ☐ Other: _____.

DETAILED ACTION

Response to Amendment

1. This action is in response to the amendment filed 10/27/2004. Claims 2-3, 8-9, 11, and 28 have been amended; claim 1 has been cancelled.

Response to Arguments

2. Applicant's arguments, see page 8, 2nd paragraph, filed 10/27/2004, with respect to the rejection(s)of claim(s) 3 under 35 U.S.C 103(a) have been fully considered and are persuasive. Therefore, the rejection has been withdrawn. However, a discovery of new prior art has necessitated new grounds of rejection. The delay in citation of the newly discovered prior art is regretted.

3. Applicant's arguments, filed 10/27/2004, with respect to the rejections of claims 1, 7-8 and 15 under 35 U.S.C 103(a) have been fully considered but they are not persuasive.

Regarding claim 1, Applicant argues that Schneier does not teach storing the key-encryption key in a protected memory that prevents subsequent modification (page 7, 6th paragraph). Schneier teaches that the long-term key-encryption key must be stored securely (page 177, 2nd paragraph) and that inherently prevents subsequent modification of the key.

Regarding claim 7, Applicant argues that Menezes does not teach transmitting the short-termed value to the second device prior to producing the secret value (page 8,

4th paragraph). Menezes discloses transmitting the short-termed value to the second device prior to producing the secret value in Protocol 12.20.

Regarding claim 8, Applicant argues that Menezes does not teach an iterative function being performed (page 8, 6th paragraph). However, Menezes discloses an iterative function being performed (p. 390, see Slowing down the password mapping).

Regarding claim 15, it was stated in the previous Office Action (page 10, last paragraph) that the session key met the limitation of a secret value, not a short-term value, see Remarks, page 9, 5th paragraph. Applicant argues that the combination of the session key with the symmetric key is not suggested, see page 9, last paragraph; however, the rejection uses the combination of a long-term value, as disclosed by Davis, and a short-term value, as taught by Menezes, to generate a secret value (page 499, section 12.20). Menezes also provides motivation for combining the references.

Claim Objections

4. Claim 10 is objected to under 37 CFR 1.75(c), as being of improper dependent form for failing to further limit the subject matter of a previous claim. Applicant is required to cancel the claim(s), or amend the claim(s) to place the claim(s) in proper dependent form, or rewrite the claim(s) in independent form. A power-up sequence does not constitute a further limitation.

Claim Rejections - 35 USC § 112

5. The following is a quotation of the second paragraph of 35 U.S.C. 112:

> The specification shall conclude with one or more claims particularly pointing out and distinctly claiming the subject matter which the applicant regards as his invention.

6. Claim 10 is rejected under 35 U.S.C. 112, second paragraph, as being indefinite for failing to particularly point out and distinctly claim the subject matter which applicant regards as the invention. Claim 10 recites the limitation "the periodic event" in line 1. There is insufficient antecedent basis for this limitation in the claim.

Claim Rejections - 35 USC § 102

7. The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

> A person shall be entitled to a patent unless –
>
> (e) the invention was described in (1) an application for patent, published under section 122(b), by another filed in the United States before the invention by the applicant for patent or (2) a patent granted on an application for patent by another filed in the United States before the invention by the applicant for patent, except that an international application filed under the treaty defined in section 351(a) shall have the effects for purposes of this subsection of an application filed in the United States only if the international application designated the United States and was published under Article 21(2) of such treaty in the English language.

8. Claim 3 is rejected under 35 U.S.C. 102(e) as being anticipated by Patel (6,327,660).

The applied reference has a common assignee with the instant application. Based upon the earlier effective U.S. filing date of the reference, it constitutes prior art under 35 U.S.C. 102(e). This rejection under 35 U.S.C. 102(e) might be overcome either by a showing under 37 CFR 1.132 that any invention disclosed but not claimed in the reference was derived from the inventor of this application and is thus not the invention "by another," or by an appropriate showing under 37 CFR 1.131.

Patel discloses within a first device, generating keying material for permanent storage in a protected area of internal memory of the first device that prevents subsequent modification of the data (col. 5, lines 45-55); and within the first device, producing an encryption key, which meets the limitation of a secret value, being a combination of both the keying material and a short term value generated in response to a periodic event, the periodic event being a power-up sequence by a platform employing the first device (col. 7, lines 13-20; col. 9, lines 48-58).

Claim Rejections - 35 USC § 103

9. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

10. Claims 3-7 are rejected under 35 U.S.C. 103(a) as being unpatentable over Schneier ("Applied Cryptography") in view of Menezes et al. ("Handbook of Applied Cryptography", Section 12.3) and Levy et al (6,212,633).

Regarding claim 3, Schneier discloses a method comprising: within a first device, generating a key-encryption key for permanent storage in a protected area of internal memory of the first device that prevents subsequent modification of the data (p. 176, 6th par., "Alice generates a key using a random-key generator"; p. 177, 2nd par., "However, since compromise ... be stored securely"); and within the first device, producing a data

key, which meets the limitation of a secret value, the data key being generated in response to a periodic event (p. 177, 2nd par., "Once Alice and Bob both ... be changed as often").

Schneier does not disclose that the secret value is a combination of both the data and a short-term value. Menezes discloses a first entity, entity B, that generates a short-term value and then generates a secret value that is a combination of a shared long-term value, and a short-term value (p. 499, 2nd par., "In the other techniques ... and key derivation"; section 12.20). It would have been obvious to one of ordinary skill in the art at the time the invention was made to modify the Schneier method such that the secret value is a combination of both the long-term value and a short-term value, as taught by Menezes. The motivation for doing so would have been a key derivation protocol which entirely avoids the use of an encryption function might offer potential advantages with respect to export restrictions (p. 499, 2nd par).

Schneier does not disclose that the periodic event being a power-up sequence. Levy discloses that new session keys, which meet the limitation of secret values, are generated in response to a power-up sequence (col. 9, lines 46-59; col. 16, lines 54-62). It would have been obvious to one of ordinary skill in the art at the time the invention was made to modify the Schneier method further to generate the secret value in response to the power-up sequence, as taught by Levy. Accordingly the short-term value is also generated in response to the power-up sequence. The motivation for doing so would have been that the encryption scheme is changed on a regular basis, thereby heightening the security for the interface.

Regarding claims 4-5, Schneier discloses transmitting the data to the second device prior to producing the secret value. Schneier does not disclose transmitting a first command from the second device to the first device prior to generating the data. However, Examiner takes Official Notice that an entity transmits a command to another entity requesting a key prior to the key being generated is conventional and well known. It would have been obvious to one of ordinary skill in the art at the time the invention was made to transmit a first command from the second device to the first device prior to generating the data since Examiner takes Official Notice that an entity transmits a command to another entity requesting a key prior to the key being generated is conventional and well known, and well known for the purpose of the other entity knowing when to generate the key and to whom the key is generated for.

Regarding claim 6, Menezes further discloses transmitting a second command from a second entity, entity A, to the first entity and generating the short-term value within the first entity in response to the second command (page 499, section 12.20). It would have been obvious to one of ordinary skill in the art at the time the invention was made to modify the Schneier method to transmit a second command from a second entity to the first entity and generate the short-term value within the first entity in response to the second command, as taught by Menezes. Please refer to motivation recited for generating a secret value within the first device, the secret value being a combination of both the long-term value and a short-term value as taught by Menezes in claim 3.

Regarding claim 7, Menezes further discloses transmitting the short-term value to a second entity prior to producing the secret value (page 499, section 12.20). It would have been obvious to one of ordinary skill in the art at the time the invention was made to modify the Schneier method to transmit the short-term value to the second device prior to producing the secret value, as taught by Menezes. Please refer to motivation recited for generating a secret value within the first device, the secret value being a combination of both the long-term value and a short-term value as taught by Menezes in claim 3.

11. Claim 8 is rejected under 35 U.S.C. 103(a) as being unpatentable over Schneier in view of Menezes and Levy as applied to claim 3 above, and further in view of Menezes ("Handbook of Applied Cryptography", Section 10.2). Menezes discloses that the combination of claim 3 is a result produced by performing a hash operation on both the data and the short-term value. However, Menezes does not disclose that the hash operation is performed successively. Menezes, in Section 10.2, discloses successively performing a hash operation (p. 390, 2nd par.). It would have been obvious to one of ordinary skill in the art at the time the invention was made to modify the method of claim 3 such that that the hash operation is performed successively, as taught by Menezes, in order to slow down attacks.

12. Claims 9-10 and 12-13 are rejected under 35 U.S.C. 103(a) as being unpatentable over Pitchenik (6,397,328) in view of Menezes et al. ("Handbook of Applied Cryptography", Sections 12.2-12.3) and Levy.

Regarding claims 9-10, Pitchenik discloses a method comprising: generating a shared secret key, which meets the limitation of a long-term value, within a first device (fig. 2, step 100); permanently storing the long-term value within a protected area of an internal memory of the first device (fig. 2, step 105); providing the long-term value to a second device communicatively coupled to the first device (fig. 2, step 110).

Pitchenik does not disclose generating a short-term value within the first device, the short-term value being modified after each power up sequence; providing the short-term value to the second device; and generating a secret value within the first device and the second device, the secret value being a combination of both the long-term value and the short-term value.

Menezes discloses a method for deriving a session key for each communications session between two entities using a long-term secret shared by the entities, the method comprising: generating a short-term value within a first entity, entity B, the short-term value being modified after each periodic event; providing the short-term value to the second device; and generating a session key, which meets the limitation of a secret value, within the first and second entities, the session key being a combination of both the long-term value and the short-term value (p. 499, section 12.20). It would have been obvious to one of ordinary skill in the art at the time the invention was made to modify the Pitchenik method to include the steps of generating a short-term value within

the first device, the short-term value being modified after each periodic event; providing the short-term value to the second device; and generating a session key within the first device and the second device, the session key being a combination of both the long-term value and the short-term value, as taught by Menezes. The use of session keys would limit available ciphertext (under a fixed key) for cryptanalyst attack (p. 494, 1st par.).

Levy discloses that new session keys, which meet the limitation of secret values, are generated in response to a power-up sequence (col. 9, lines 46-59; col. 16, lines 54-62). It would have been obvious to one of ordinary skill in the art at the time the invention was made to modify the Pitchenik method further to generate the secret value in response to the power-up sequence, as taught by Levy. Accordingly the short-term value is also generated in response to the power-up sequence. The motivation for doing so would have been that the encryption scheme is changed on a regular basis, thereby heightening the security for the interface.

Regarding claim 12, Pitchenik further discloses that the long-term value is generated in response to an initial power-up sequence when the first device is in communication with the second device (fig. 2).

Regarding claim 13, Menezes further discloses transmitting a second command from the first entity to the second entity prior to generating the short-term value (p. 499, section 12.20). It would have been obvious to one of ordinary skill in the art at the time the invention was made to modify the Schneier method to transmit a second command from the first entity to the second entity prior to generating the short-term value, as

taught by Menezes. Please refer to motivation recited for generating and utilizing session keys as taught by Menezes in claim 9.

13. Claim 11 is rejected under 35 U.S.C. 103(a) as being unpatentable over Pitchenik in view of Menezes and Levy as applied to claim 9 above, and further in view of Burns ("INTEL: Intel introduces new chipset for intel Pentium III processor-based performance PCs").

Pitchenik does not disclose transmitting a first command from the second device to the first device prior to generating the long-term value, which is the shared secret key. However, Examiner takes Official Notice that an entity transmits a command to another entity requesting a key prior to the key being generated is conventional and well known. It would have been obvious to one of ordinary skill in the art at the time the invention was made to transmit a first command from the second device to the first device prior to generating the long-term value since Examiner takes Official Notice that an entity transmits a command to another entity requesting a key prior to the key being generated is conventional and well known, and well known for the purpose of the other entity knowing when to generate the key and to whom the key is generated for.

Pitchenik does not disclose that the first device is a trusted platform module (TPM) and the second device is an input/output control hub (ICH). Davis discloses a cryptographic device, which meets the limitation of a trusted platform module (TPM), securely communicates with a chipset using a secret value, the secret value being a session key. It would have been obvious to one of ordinary skill in the art at the time the

invention was made to modify the Pitchenik method such that the first device is a trusted platform module (TPM) securely communicates with a chipset using a secret value, as taught by Davis. The motivation for doing so would have been to optimize performance of an electronic system during cryptographic operations (col. 2, lines 31-42).

Pitchenik does not disclose an input/output control hub (ICH). Burns discloses a chipset comprising an ICH ("This revolutionary chipset architecture ... and a Firmware Hub"). It would have been obvious to one of ordinary skill in the art at the time the invention was made to modify the Pitchenik method further such that the second device is an ICH, as taught by Burns. The ICH includes an Alert on LAN feature that allows a non-booting system to send a status update to the network administrator even when the microprocessor is not present.

14. Claim 14 is rejected under 35 U.S.C. 103(a) as being unpatentable over Pitchenik in view of Menezes as applied to claim 9 above, and further in view of Menezes ("Handbook of Applied Cryptography", Section 10.2). Menezes discloses that the secret value of claim 9 is a result produced by performing a hash operation on both the data and the short-term value. However, Menezes does not disclose that the hash operation is performed successively. Menezes, in Section 10.2, discloses successively performing a hash operation (p. 390, 2nd par.). It would have been obvious to one of ordinary skill in the art at the time the invention was made to modify the method of claim

9 such that that the hash operation is performed successively, as taught by Menezes, in order to slow down attacks.

15. Claims 15-16 and 18 are rejected under 35 U.S.C. 103(a) as being unpatentable over Davis (5,818,939) in view of Menezes ("Handbook of Applied Cryptography", Section 12.3) and Burns ("INTEL: Intel introduces new chipset for intel Pentium III processor-based performance PCs").

Regarding claims 15-16, Davis discloses a platform comprising: a link (fig. 4, element 330); a chipset coupled to the link (fig. 4, element 315); and a cryptographic device, which meets the limitation of a trusted platform module (TPM), coupled to the link (fig. 4, element 335), the cryptographic coprocessor including a package (fig. 4, element 335), a asymmetric key generation unit contained within the packet to generate a shared secret key, which meets the limitation of a long term value (col. 5, lines 24-36; col. 6, lines 57-65); and an internal memory contained within the package, the internal memory to permanently store the shared secret key (fig. 4, element 610) and to temporarily store a session key, which meets the limitation of a secret value (col. 6, lines 25-28).

Davis does not disclose an input/output control hub (ICH). Burns discloses a chipset comprising an ICH ("This revolutionary chipset architecture ... and a Firmware Hub"). It would have been obvious to one of ordinary skill in the art at the time the invention was made to modify the Davis platform to use a chipset comprising an ICH, as taught by Burns. The ICH includes an Alert on LAN feature that allows a non-booting

system to send a status update to the network administrator even when the microprocessor is not present.

Davis does not disclose that the asymmetric key generation unit generates a short-term value and the session key being a combination of the shared secret key and the short-term value. Menezes discloses a device that has a long-term shared secret key (p. 497, "Point-to-point key update ... a priori by two parties A and B"); and the device generates a short-term value and a session key, which meets the limitation of a secret value, the session key being a combination of the shared secret key and the short-term value (p. 499, section 12.20). It would have been obvious to one of ordinary skill in the art at the time the invention was made to modify the Davis platform such that the asymmetric key generation unit generates a short-term value and a secret value being a combination of the shared secret key and the short-term value, as taught by Menezes. The motivation for doing so would have been that a key derivation protocol which entirely avoids the use of an encryption function might offer potential advantages with respect to export restrictions (p. 499, 2nd par.).

Regarding claim 18, Davis further discloses that the asymmetric key generation unit includes a number generator (fig. 4, element 620).

16. Claim 17 is rejected under 35 U.S.C. 103(a) as being unpatentable over Davis ('939), Menezes and Burns as applied to claim 16 above, and further in view of Davis (5,949,881). Davis ('939) discloses that the cryptographic device transmits the shared secret key to the chipset over the link during manufacture of the platform (col. 5, lines

24-36; col. 6, lines 6-30); however, Davis does not disclose that the cryptographic device transmits the shared secret key to the ICH over the link during manufacture of the platform and transmits the short term value to the ICH over the link in response to a power-up sequence by the platform. Davis ('881) discloses a platform comprising a cryptographic device and an I/O controller, which meets the limitation of an ICH (fig. 1, elements 130 and 151). Davis further discloses that the cryptographic device and the I/O controller share a secret key (fig. 1; col. 3, lines 25-29), and that the cryptographic device generates and uses a session key, in addition to the symmetric key, to authenticate and activate the platform in response to a power-up sequence by the platform (fig. 2; col. 3, lines 13-16). It would have been obvious to one of ordinary skill in the art at the time the invention was made to modify the platform of claim 16 such that the cryptographic device generates and uses a session key, in addition to the symmetric key, to authenticate and activate the platform in response to a power-up sequence by the platform, as disclosed by Davis in reference '881. Accordingly, the cryptographic device needs to transmit the long-term value to the ICH over the link during manufacture of the platform and transmit the short-term value to the ICH over the link in response to a power-up sequence by the platform. The motivation for doing so would have been to reduce the value of a laptop computer in the event of its theft or loss and thus, in effect, would deter such theft and encourage its return in the event of loss (col. 1, lines 53-57).

17. Claim 19 is rejected under 35 U.S.C. 103(a) as being unpatentable over Davis, Menezes and Burns as applied to claim 15 above, and further in view of Menezes ("Handbook of Applied Cryptography", Section 10.2). Menezes (p. 499, section 12.20) discloses that the secret value is a result produced by performing a hash operation on both the long-term value and the short-term value. However, Menezes does not disclose that the hash operation is performed successively. Menezes, in Section 10.2, discloses successively performing a hash operation (p. 390, 2nd par.). It would have been obvious to one of ordinary skill in the art at the time the invention was made to modify the method of claim 15 such that that the hash operation is performed successively, as taught by Menezes, in order to slow down attacks.

18. Claims 20, 22-23, 25-26 and 28 are rejected under 35 U.S.C. 103(a) as being unpatentable over Davis (5,819,939) in view of Menezes (Section 12.3).

Regarding claims 20 and 25-26, Davis discloses a device comprising: an internal memory (fig. 4, element 610); an asymmetric key generation unit to generate, in response to an initial event, a unique long-term value for permanent storage in a protected area of the internal memory (col. 5, lines 24-36; col. 6, lines 57-65).

Davis further discloses that the asymmetric key generation unit generates a session key, which meets the limitation of a secret value; however, Davis does not disclose that the asymmetric key generation unit generates, in response to a periodic event, a short-term value for storage in the internal memory and a cryptographic engine to produce the session key by combining both the long-term value and the short-term

value. Menezes discloses a key generation unit for deriving a session key, which meets the limitation of a secret value, by generating, in response to a periodic event, a short-term value for storage in the internal memory; and a cryptographic engine to produce the session key by combining both the long-term value and the short-term value (p. 499, section 12.20). It would have been obvious to one of ordinary skill in the art at the time the invention was made to modify the Davis device such that the asymmetric key generation unit generates, in response to a periodic event, a short-term value for storage in the internal memory and a cryptographic engine to produce a secret value by combining both the long-term value and the short-term value, as taught by Menezes. The motivation for doing so would have been that a key derivation protocol which entirely avoids the use of an encryption function might offer potential advantages with respect to export restrictions (p. 499, 2nd paragraph).

Regarding claim 22, Davis further discloses that the initial event includes an initial power-up sequence of the device when in communication with another device of the platform for which the secret value is generated to create one secure communication channel between the devices (col. 5, lines 24-36; col. 6, lines 6-30).

Regarding claim 23, Davis further discloses that the internal memory includes a non-volatile memory (fig. 4, element 610) and a volatile memory (fig. 4, element 615).

Regarding claim 28, Davis further discloses that the initial event includes an initial power-up sequence performed during assembly of the platform (col. 5, lines 24-36).

19. Claims 21 and 27 are rejected under 35 U.S.C. 103(a) as being unpatentable over Davis in view of Menezes as applied to claims 20 and 25 above, and further in view of Levy. Davis and Menezes do not disclose that the periodic event includes a power-up sequence. Levy discloses that new session keys, which meet the limitation of secret values, are generated in response to a power-up sequence (col. 9, lines 46-59; col. 16, lines 54-62). It would have been obvious to one of ordinary skill in the art at the time the invention was made to modify the Pitchenik method further to generate the secret value in response to the power-up sequence, as taught by Levy. Accordingly the short-term value is also generated in response to the power-up sequence. The motivation for doing so would have been that the encryption scheme is changed on a regular basis, thereby heightening the security for the interface.

20. Claim 24 is rejected under 35 U.S.C. 103(a) as being unpatentable over Davis in view of Menezes as applied to claim 20 above, and further in view of Menezes (Section 10.2). Menezes (p. 499, section 12.20) discloses that the secret value is a result produced by performing a hash operation on both the long-term value and the short-term value. However, Menezes does not disclose that the hash operation is performed successively. Menezes, in Section 10.2, discloses successively performing a hash operation (p. 390, 2nd par.). It would have been obvious to one of ordinary skill in the art at the time the invention was made to modify the method of claim 20 such that that the hash operation is performed successively, as taught by Menezes, in order to slow down attacks.

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Minh Dinh whose telephone number is 571-272-3802. The examiner can normally be reached on Mon-Fri: 10:00am-6:30pm.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Gilberto Barron can be reached on 571-272-3799. The fax phone number for the organization where this application or proceeding is assigned is 703-872-9306.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

MD

Minh Dinh
Examiner
Art Unit 2132

MD
2/21/05

Gilberto Barron

GILBERTO BARRON JR.
SUPERVISORY PATENT EXAMINER
TECHNOLOGY CENTER 2100